TITLE:

The Codes and the Lattices of Hadamard Matrices (Finite Groups and Algebraic Combinatorics)

AUTHOR(S):

Munemasa, Akihiro; Tamura, Hiroki

CITATION:

Munemasa, Akihiro ...[et al]. The Codes and the Lattices of Hadamard Matrices (Finite Groups and Algebraic Combinatorics). 数理解析研究所講究録 2008, 1593: 154-161

ISSUE DATE:

2008-04

URL:

http://hdl.handle.net/2433/81645

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録
第1593巻 2008年 154-161

The Codes and the Lattices of Hadamard Matrices

Akihiro Munemasa and Hiroki Tamura
Graduate School of Information Sciences
Tohoku University

It has been observed by Assmus and Key as a result of the complete classification of Hadamard matrices of order 24, that the extremality of the binary code of a Hadamard matrix H of order 24 is equivalent to the extremality of the ternary code of H^T. In this note, we present two proofs of this fact, neither of which depends on the classification. One is a consequence of a more general result on the minimum weight of the dual of the code of a Hadamard matrix. The other relates the lattices obtained from the binary code and from the ternary code. Both proofs are presented in greater generality to include higher orders. In particular, the latter method is also used to show the equivalence of (i) the extremality of the ternary code, (ii) the extremality of the $\mathbb{Z}_4$-code, and (iii) the extremality of a lattice obtained from a Hadamard matrix of order 48.

1 Minimum weights of codes of Hadamard matrices

We denote the all-ones matrix by J, and the all-ones vector by $\mathbf{1}$. A Hadamard matrix H is said to be normalized if its first row is $\mathbf{1}$. We also denote by e_i the vector with a 1 in the i-th coordinate and 0 elsewhere.

Lemma 1. *Let H be a Hadamard matrix of order n, m an integer such that $m|n$ and $(m, n/m) = 1$. Then the row vectors of H generate a self-dual code of length n over $\mathbb{Z}/m\mathbb{Z}$.*

Let m be a positive integer, and set $V = \mathbb{Z}/m\mathbb{Z}$. We regard an element $u \in V$ as an element of the set of integers $\{0, 1, \ldots, m-1\}$, and define the

Lee weight and the Euclidean norm of an element $u \in V$ by

$$\begin{aligned} \mathrm{Lee}(u) &= \min\{u, m-u\}, \\ \mathrm{Norm}(u) &= (\mathrm{Lee}(u))^2. \end{aligned}$$

For a vector $u = (u_1, \ldots, u_n) \in V^n$, we set

$$\mathrm{Norm}(u) = \sum_{i=1}^{n} \mathrm{Norm}(u_i).$$

Alternatively, the Euclidean norm can be defined as

$$\mathrm{Norm}(u) = \min\left\{ \|v\|^2 \mid v \in \mathbb{Z}^n, v \bmod m = u \right\}.$$

Recall that a self-dual code over $\mathbb{Z}/2m\mathbb{Z}$ is type II if it contains $\mathbf{1}$ and the Euclidean norm of every codeword is divisible by $4m$.

Lemma 2. *Let H be a normalized Hadamard matrix of order n, $B = \frac{1}{2}(H + J)$ the binary Hadamard matrix associated to H. Let m be an integer such that $8m|n$ and $(2m, n/8m) = 1$. Then the row vectors of B generate a type II self-dual code over $\mathbb{Z}/2m\mathbb{Z}$ of length n.*

We introduce two types of pair of norms of a vector over $V = \mathbb{Z}/mZ$. When m is odd, we define the odd norm and the even norm by

$$\begin{aligned} \mathrm{Norm}_o(u) &= \min\left(\left\{ \|v\|^2 \mid v \in \mathbb{Z}^n,\ v \bmod m = u \right\} \cap (1 + 2\mathbb{Z})\right), \\ \mathrm{Norm}_e(u) &= \min\left(\left\{ \|v\|^2 \mid v \in \mathbb{Z}^n,\ v \bmod m = u \right\} \cap 2\mathbb{Z}\right). \end{aligned}$$

We also define type I norm and type II norm for an integer m and $u \in \mathbf{1}^{\perp} \subset V^n$ by

$$\begin{aligned} \mathrm{Norm}_I(u) &= \min\left\{ \|v\|^2 \mid v \in \mathbb{Z}^n,\ v \bmod m = u,\ v \cdot \mathbf{1} \equiv m \pmod{2m} \right\}, \\ \mathrm{Norm}_{II}(u) &= \min\left\{ \|v\|^2 \mid v \in \mathbb{Z}^n,\ v \bmod m = u,\ v \cdot \mathbf{1} \equiv 0 \pmod{2m} \right\}. \end{aligned}$$

When m is odd, type I (resp. type II) norm coincide with odd (resp. even) norm. Note that if $u = v \bmod m$ and $\mathrm{Norm}(u) = \|v\|^2$, then

$$\begin{aligned} &\{\mathrm{Norm}_o(u), \mathrm{Norm}_e(u)\}, \{\mathrm{Norm}_I(u), \mathrm{Norm}_{II}(u)\} \\ &= \{\|v\|^2, \min_i\{\|v \pm me_i\|^2\}\} \\ &= \{\mathrm{Norm}(u), \mathrm{Norm}(u) + m(m - 2\max_i\{\mathrm{Lee}(u_i)\})\}. \end{aligned}$$

Let H be a normalized Hadamard matrix of order n, and let B be the binary Hadamard matrix associated to H. Let C_m be the code over $\mathbb{Z}/m\mathbb{Z}$ generated by the rows of H^T, and C'_l the code over $\mathbb{Z}/l\mathbb{Z}$ generated by the rows of B, where $m \geq 3$ is an odd integer and $l \geq 2$ is an integer.

Lemma 3. (i) *$C_m^{\perp}$ has no codeword of odd norm less than m^2,*

(ii) *$C_l'^{\perp}$ has no codeword of type I norm less than l^2,*

Proof. (i) Let v be a vector in $\mathbb{Z}^n$ such that $v \bmod m = u \in C_m^{\perp}$ and $\|v\|^2 = \mathrm{Norm}_o(u)$. Then we have $vH^T \equiv 0 \pmod m$ and $vH^T \equiv v\mathbf{1}^T\mathbf{1} \equiv \mathbf{1} \pmod 2$ and thus $vH^T \equiv m\mathbf{1} \pmod{2m}$. So we have $\|v\|^2 = vH^THv^T/n = \|vH^T\|^2/n \geq m^2$. (ii) is similar. □

Theorem 4. *If l and m satisfy $(l,m) = 1$ and $n \equiv 0 \pmod{4lm}$, then the following statements hold.*

(i) *If $C_m^{\perp}$ has a codeword of even norm d and odd norm m^2+k, then C_l' has a nonzero codeword of type II norm at most $dn/4m^2$ when $d < 2lm$ or $k < d(l-1)/l$, and exactly $dn/4m^2$, which is also the Euclidean norm, when $d < 2\lfloor (l+2)/2 \rfloor m$ or $k = 0$.*

(ii) *If $C_l'^{\perp}$ has a codeword of type II norm d and type I norm l^2+k, then C_m has a nonzero codeword of even norm at most $dn/4l^2$ when $d < 2lm$ or $k < d(m-1)/m$, and exactly $dn/4l^2$, which is also the Euclidean norm, when $d < l(m+1)$ or $k = 0$.*

Proof. (sketch) (i) If $C_m^{\perp}$ has such a codeword, then there exists a vector $v \in \mathbb{Z}^n$ satisfying $vH \equiv 0 \pmod{2m}$, $\|v\|^2 = d$ and $\|v - me_i\|^2 = m^2+k$ for some i. Since $(l,m) = 1$, there exists an integer t such that $mt \equiv 1 \pmod l$, and $(1/2m)vH \equiv t(vB - (v\cdot\mathbf{1}/2)\mathbf{1}) \pmod l$. Thus $(1/2m)vH \bmod l$ is a codeword of C_l' which has Euclidean norm at most $\|(1/2m)vH\|^2 = (1/2m)^2 vHH^Tv^t = dn/4m^2$, and since $(1/2m)vH\mathbf{1}^T = (n/2m)v_1 \equiv 0 \pmod{2l}$, type II norm also. Under the given conditions, we have $(1/2m)vH \bmod l \neq 0$. (ii) is shown by the similar argument as (i). □

In particular, when $m = 3$, $l = 2$ and $n = 24$, we have the following.

Corollary 5. *Let H be a normalized Hadamard matrix of order 24. Then C_3 is an extremal self-dual $[24, 12, 9]$ code if and only if C_2' is an extremal doubly even self-dual binary $[24, 12, 8]$ code.*

Proof. By Lemmas 1 and 2, C_3 is self-dual while C_2' is doubly even self-dual. Theorem 4 implies that C_3 has a codeword of weight 6 if and only if C_2' has a codeword of weight 4, or equivalently, C_2' is non-extremal. Since C_3 has no codeword of weight 3 by Lemma 3 (ii), the former condition is equivalent to C_3 being non-extremal. □

When $m = 3$, $l = 4$ and $n = 48$, we have:

Corollary 6. *Let H be a normalized Hadamard matrix of order 48. Then C_3 is an extremal self-dual $[48, 24, 15]$ code if and only if C_4' has minimum type II norm 24.*

In fact, C_4' with minimum type II norm 24 has minimum Euclidean norm 24. This will be shown in later.

It is known that there are at least two inequivalent extremal ternary self-dual code of length 48, the quadratic residue code and the Pless symmetry code. The codewords of weight 48 in these codes constitute the rows and their negatives of a Hadamard matrix. ([4, §2.8, §2.10 of Chap. 3]).

2 Lattices

Let C be a code of length n over $\mathbb{Z}/m\mathbb{Z}$ with generator matrix M. We regard the entries of H as integers, and let $\mathbb{Z}^k M$ denote the row $\mathbb{Z}$-module of M, that is, the set of $\mathbb{Z}$-linear combinations of the row vectors of M, where k is the number of rows of M. The lattice $A(C)$ of the code C is defined as $A(C) = \frac{1}{\sqrt{m}}\mathbb{Z}^{k+n}\begin{bmatrix} M \\ mI \end{bmatrix}$, and $A(C)$ is integral (resp. unimodular, even unimodular) if and only if C is self-orthogonal (resp. self-dual, type II).

Let $m \geq 3$ be an odd integer, l an integer such that $(l, m) = 1$, H a normalized Hadamard matrix of order $n = 4lm$. Then by Lemmas 1 and 2, the code C_m over $\mathbb{Z}/m\mathbb{Z}$ and the code C_l' over $\mathbb{Z}/l\mathbb{Z}$ are self-dual, and thus $A(C_m) = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n}\begin{bmatrix} H^T \\ mI \end{bmatrix}$ and $A(C_l') = \frac{1}{\sqrt{l}}\mathbb{Z}^{2n}\begin{bmatrix} B \\ lI \end{bmatrix}$ are both unimodular, the former is odd, and the latter is even if and only if l is even.

In the following, we assume H and H^T are both normalized. Then we have

$$A(C_m) = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n}\begin{bmatrix} B^T \\ mI \end{bmatrix},$$

so the even sublattice of $A(C_m)$ is

$$B(C_m) = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n}\begin{bmatrix} B^T \\ m(I + \mathbf{1}^T e_1) \end{bmatrix}.$$

There are two unimodular lattices containing $B(C_m)$, other than $A(C_m)$. One is the copy of $A(C_l')$, and we denote the other by $\Lambda(C_m)$. Observe that

$$\times\frac{1}{\sqrt{n}}H$$

$$A(C_m) = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n}\begin{bmatrix} B^T \\ mI \end{bmatrix} \quad \frac{1}{\sqrt{l}}\mathbb{Z}^{2n+1}\begin{bmatrix} B \\ l(I+\mathbf{1}^T e_1) \\ \frac{1}{2}\mathbf{1} \end{bmatrix}$$

$$\frac{1}{\sqrt{m}}\mathbb{Z}^{2n+1}\begin{bmatrix} B^T \\ m(I+\mathbf{1}^T e_1) \\ \frac{1}{2}\mathbf{1} \end{bmatrix} \quad \frac{1}{\sqrt{l}}\mathbb{Z}^{2n}\begin{bmatrix} B \\ lI \end{bmatrix} = A(C_l')$$

$$B(C_m) = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n}\begin{bmatrix} B^T \\ m(I+\mathbf{1}^T e_1) \end{bmatrix} \quad \frac{1}{\sqrt{l}}\mathbb{Z}^{2n}\begin{bmatrix} B \\ l(I+\mathbf{1}^T e_1) \end{bmatrix} = B(C_l')$$

$$\Lambda(C_m) = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n+1}\begin{bmatrix} B^T \\ m(I+\mathbf{1}^T e_1) \\ me_1+\frac{1}{2}\mathbf{1} \end{bmatrix} \quad \frac{1}{\sqrt{l}}\mathbb{Z}^{2n+1}\begin{bmatrix} B \\ l(I+\mathbf{1}^T e_1) \\ le_1+\frac{1}{2}\mathbf{1} \end{bmatrix} = \Lambda(C_l')$$

$$\times\frac{1}{\sqrt{n}}H^T$$

The relation between $A(C_m)$, $A(C_l')$ and $B(C_m)$, $B(C_l')$ is given as

$$B(C_m) = \{x \in A(C_m) \mid \|x\|^2 \equiv 0 \pmod 2\}$$
$$B(C_l') = \{x \in A(C_l') \mid \frac{1}{\sqrt{l}}x \cdot 1 \equiv 0 \pmod 2\}.$$

Since $\min(\frac{1}{\sqrt{m}}\mathbb{Z}^n\left[m(I+\mathbf{1}^T e_1)\right]) = 2m$ and $\min(\frac{1}{\sqrt{l}}\mathbb{Z}^n\left[l(I+\mathbf{1}^T e_1)\right]) = 2l$, we have

$$\min B(C_m) = \min\{2m, \frac{1}{m}\min_{u\in C_m\setminus\{0\}}\mathrm{Norm}_e(u)\}$$
$$= \min\{2l, \frac{1}{l}\min_{u\in C_l'\setminus\{0\}}\mathrm{Norm}_{II}(u)\}.$$

We also have $\Lambda(C_m) \setminus B(C_m) \subset \frac{1}{2\sqrt{m}}(1+2\mathbb{Z})^n$ and $\Lambda(C_l') \setminus B(C_l') \subset \frac{1}{2\sqrt{l}}(1+2\mathbb{Z})^n$, and thus $\min(\Lambda(C_m)\setminus B(C_m)) \geq \max\{l, m\}$. If $l \equiv 0 \pmod 2$, $\Lambda(C_m)$ is an even lattice, so $\min(\Lambda(C_m) \setminus B(C_m)) \geq \max\{l, m+1\}$.

Thus we have the following.

Theorem 7. *Let $d = \min\{2l, 2m\}$, then the following statements* (i)–(iii) *are equivalent, moreover if $d \leq \max\{l, m+\delta_{l \bmod 2,0}\}$,* (iii) *and* (iv) *are equivalent:*

(i) C_m *has minimum even norm at least* dm,

(ii) C_l' *has minimum type II norm at least* dl,

(iii) $B(C_m)$ *has minimum norm* d,

(iv) $\Lambda(C_m)$ *has minimum norm* d.

Note that the minimum even norm of C_m and minimum type II norm of C_l' are both at most $n/2$, as the binary Hadamard matrix has a row of weight $n/2$.

Let $(l, m) = (2, 3)$ and $(4, 3)$. Then we have another proofs of Corollaries 5 and 6.

Corollary 8. *Let* H *be a normalized Hadamard matrix of order* 24. *The following statements are equivalent:*

(i) C_3 *has minimum weight* 9,

(ii) C_2' *has minimum weight* 8,

(iii) $\Lambda(C_3)$ *has minimum norm* 4 *(hence is isomorphic to the Leech lattice).*

Corollary 9. *Let* H *be a normalized Hadamard matrix of order* 48. *The following statements are equivalent:*

(i) C_3 *has minimum weight* 15,

(ii) C_4' *has minimum type II norm* 24,

(iii) $B(C_3)$ *has minimum norm* 6.

As a matter of fact, we have stronger result by the following argument.

Lemma 10. *The number of vectors of* $\Lambda(C_m) \setminus B(C_m)$ *and* $A(C_l') \setminus B(C_l')$ *of minimum norm* l *is equal to the number of codewords of* C_m *of odd (resp. even) weight whose nonzero entries are all equal to* 1. *The latter is at least* $2n$ *and exactly* $2n$ *if and only if the minimum type I norm of* $C_l' \setminus \{0\}$ *is larger than* l^2.

Proof. We have $A(C_l') \setminus B(C_l') \cong B(C_m) - (1/2\sqrt{m})\mathbf{1}$ and $\Lambda(C_m) \setminus B(C_m) = B(C_m) - (1/\sqrt{m})(me_1 + \frac{1}{2}\mathbf{1})$. Their norm l vectors are of the form $v' = (1/2\sqrt{m})(\pm 1, \ldots, \pm 1)$, and $v' + (1/2\sqrt{m})\mathbf{1} = (1/\sqrt{m})v$, $v \in \{0,1\}^n$ is obtained from a codeword of C_m. If the weight of v mod m is even, $(1/\sqrt{m})v$ belongs to $B(C_m)$ and thus v' belongs to the copy of $A(C_l') \setminus B(C_l')$, otherwise belongs to $\Lambda(C_m) \setminus B(C_m)$. A codeword of C_l' with type I norm l^2 gives norm l vectors of $A(C_l') \setminus B(C_l')$ and in particular, $0 \in C_l'$ gives the $2n$ vectors $\pm\sqrt{l}e_i$ $(i = 1, \ldots, n)$. □

Lemma 11. *Codewords of extremal ternary self-dual codes of length* 48 *with all-ones vector whose nonzero entries are all equal to* 1 *are exactly* 1 *codeword of weight* 0, 94 *of weight* 24 *and* 1 *of weight* 48.

Proof. By [10], the complete weight enumerator $W_c(x, y, z)$ of a ternary self-dual code C with all-ones vector lies in the ring $\mathbb{C}[\alpha_{12}, \beta_6^2, \pi_9^4] \oplus \beta_6 \pi_9^2 \mathbb{C}[\alpha_{12}, \beta_6^2, \pi_9^4]$ where

$$\begin{aligned}
\beta_6 &= x^6 + y^6 + z^6 - 10(x^3y^3 + y^3z^3 + z^3x^3), \\
\pi_9 &= (x^3 - y^3)(y^3 - z^3)(z^3 - x^3), \\
\alpha_{12} &= \sum x^{12} + 4\sum x^9(y^3 + z^3) + 6\sum x^6y^6 + 228\sum x^6y^3z^3,
\end{aligned}$$

where the sums are to be taken over the cyclic permutations of x, y, z. Under the assumption that the coefficients of the terms $x^{48-i-j}y^iz^j$ $(0 < i + j \leq 12)$ are 0, and that all the coefficients are non-negative, in particular of the terms $x^{33}y^{15}$ and $x^{30}y^{18}$, the complete weight enumerator of an extremal ternary self-dual $[48, 24, 15]$ code is uniquely determined to

$$\sum x^{48} + 94\sum x^{24}y^{24} + (xyz)^3 \sum a_{ijk}x^iy^jz^k$$

given in [8, Table 1]. □

A type II self-dual code over $\mathbb{Z}/4\mathbb{Z}$ of length 48 has minimum Euclidean norm at most 24 ([3] Corollary 13), and an 48-dimensional even unimodular lattice has minimum norm at most 6. Recall that an extremal ternary self-dual code of length 48 has minimum 15. By Corollary 9 and Lemmas 10 and 11, we have the following.

Theorem 12. *Let H be a normalized Hadamard matrix of order* 48. *The following statements are equivalent:*

(i) C_3 *is extremal,*

(ii) C_4' *is norm-extremal,*

(iii) $\Lambda(C_3)$ *is extremal.*

The following is an analogue of [9, Theorem 5].

Theorem 13. *Every extremal ternary self-dual code of length* 48 *is generated by a Hadamard matrix.*

Proof. It is enough to show that the 96 codewords of weight 48 of a ternary self-dual $[48, 24, 15]$ code C constitute the rows and their negatives of a Hadamard matrix of order 48. Define $u * v$ where $u = (u_1, \ldots, u_{48})$ and $v = (v_1, \ldots, v_{48})$ by $(u_1 v_1, \ldots, u_{48} v_{48})$, and define $C * v := \{u * v \mid u \in C\}$. If $v, v' \in C$ are codewords of weight 48 such that $v \neq \pm v'$, then $C * v$ is a ternary self-dual $[48, 24, 15]$ code with all-ones vector and $v' * v \neq \pm \mathbf{1}$ has weight 48. Thus $v' * v - \mathbf{1}$, and hence $v' - v$, has weight 24 by Lemma 11. □

References

[1] E. F. Assmus, Jr. and J. D. Key, "Designs and Their Codes," Cambridge University Press, Cambridge, 1992.

[2] E. Bannai, S. T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices, and invariant rings, IEEE Trans. Inform. Theory 45 (1999), 1194–1205.

[3] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, Type II Codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 43 (1997), 969–976.

[4] J. H. Conway and N. J. A. Sloane, "Sphere Packing, Lattices and Groups," 3rd ed., Springer-Verlag, New York, 1999.

[5] N. Ito, J. S. Leon and J. Q. Longyear, The 24-dimensional Hadamard matrices and their automorphism groups, unpublished.

[6] N. Ito, J. S. Leon and J. Q. Longyear, Classification of 3-(24, 12, 5) designs and 24-dimensional Hadamard matrices, J. Combin. Theory, Ser. A, 31 (1981), 66–93.

[7] H. Kimura, New Hadamard matrix of order 24, Graphs Combin. 5 (1989), 235–242.

[8] H. Koch, The 48-dimensional analogues of the Leech lattice, Proc. Steklov Inst. Math. 208 (1995), 172–178.

[9] J. S. Leon, V. Pless and N. J. A. Sloane, On ternary self-dual codes of length 24, IEEE Trans. Inform. Theory 27 (1981), 176–180.

[10] C. L. Mallows and N. J. A. Sloane, Weight enumerators of self-orthogonal codes over $GF(3)$, SIAM J. Algebr. Discr. Meth. 2 (1981), 452–480.